

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information associated with the email address
wtedh78@yahoo.com that is stored at Oath Holdings
Inc.

Case No.

3:20 mj 106

FILED
RICHARD W. NAGEL
CLERK OF COURT

2020 FEB 25 AM 11:38

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
DAYTON, OHIO

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A-3located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B-3

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

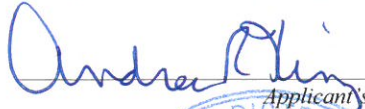
Code Section

See Attachment C-3

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature
Andrea R. Kinzig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/25/20

City and state: Dayton, Ohio


Judge's signature
Michael J. Newman, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-3

Information associated with the email address wtedh78@yahoo.com that is stored at premises controlled by Oath Holdings Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California, 94089.

ATTACHMENT B-3
Particular Things to be Seized

I. Information to be disclosed by Oath Holdings Inc. (the “Provider”)

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. The types of service utilized;
4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Cloyo Road, Centerville, Ohio, 45459.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 2251(a) and (e) (production of child pornography), 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography); involving WILLIAM THEODORE HALL during the period of January 1, 2018 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, distribution, and production of child pornography.
2. Any visual depictions of minors, and any identifying information for these minors.
3. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
4. Any communications with minors, and any identifying information for these minors.
5. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
6. Evidence of utilization of telephone accounts;
7. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
8. Any information related to the use of aliases.
9. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-3

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child pornography and child exploitation offenses committed by WILLIAM THEODORE HALL, commonly known as “TED” (hereinafter referred to as “HALL”). This Affidavit is submitted in support of Applications for search warrants for the following:
 - a. Information associated with the cellular telephone assigned call number **937-381-7919** that is stored at premises controlled by Sprint Corporation, a wireless telephone service provider headquartered at 6480 Sprint Parkway, Overland Park, Kansas, 66251 (hereinafter referred to as the “**TARGET CELL PHONE**” and more fully described in Attachment A-1);
 - b. Information associated with the Facebook account with the account name of **RitABee78** that is stored at premises controlled by Facebook Inc. (as more fully described in Attachment A-2); and
 - c. Information associated with the email address wtedh78@yahoo.com that is stored at premises controlled by Oath Holdings Inc. (as more fully described in Attachment A-3).
3. The purpose of the Applications is to seize evidence of violations of the following:
 - a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography;

- b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce; and
 - c. 18 U.S.C. § 2251(a) and (e), which make it a crime to produce or attempt to produce child pornography.
- 4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-3 hereto and are incorporated by reference.
 - 5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
 - 6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 through A-3).
 - 7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), and 2251(a) and (e) are present within the information associated with the above noted accounts (as described in Attachments A-1 through A-3).

JURISDICTION

- 8. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

- 9. 18 U.S.C. § 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of

producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

10. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
11. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
12. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
13. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign

commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

14. The following definitions apply to this Affidavit and Attachments B-1 through B-3 to this Affidavit:
- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, anal-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
 - e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By

using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

- f. An “**Internet Protocol address**”, also referred to as an “**IP address**”, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- g. “**Hyperlink**” (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- h. “**Website**” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- i. “**Uniform Resource Locator**” or “**Universal Resource Locator**” or “**URL**” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- j. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting),

photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Email Accounts

15. Oath Holdings Inc. is a company based in Sunnyvale, California. In my training and experience, I have learned that Oath Holdings Inc. provides a variety of online services, including electronic mail ("email") access, to the public.
16. Oath Holdings Inc. allows subscribers to obtain email accounts at the domain name yahoo.com, like the accounts listed in Attachment A-3. Subscribers obtain accounts by registering with Oath Holdings Inc. During the registration process, Oath Holdings Inc. asks subscribers to provide basic personal information. Therefore, the computers of Oath Holdings Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Oath Holdings Inc. subscribers) and information concerning subscribers and their use of Oath Holdings Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
17. In general, emails that are sent to Oath Holdings Inc. subscribers are stored in the subscriber's "mail box" on Oath Holdings Inc.'s servers until the subscriber deletes the email. If the subscriber does not delete the message, the messages can remain on Oath Holdings Inc.'s servers indefinitely. Even if the subscriber deletes an email, it may continue to be available on Oath Holdings Inc.'s servers for a certain period of time.
18. Oath Holdings Inc. subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Oath Holdings Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
19. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such

information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

20. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.
21. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
22. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand

the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

Facebook

23. Facebook Inc. is a company based in Menlo Park, California. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.
24. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact email addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.
25. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.
26. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other

account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

27. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.
28. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.
29. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.
30. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.
31. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.
32. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

33. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.
34. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.
35. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.
36. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.
37. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.
38. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity

can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

39. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

Telegram Messenger

40. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.
41. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.
42. Messages and media in Telegram are client-server encrypted and stored on servers by default. Telegram’s special “secret” chats use end-to-end encryption, leaving no trace of the chat’s on Telegram’s servers. The secret chats provide users the option to self-destruct messages and prohibit users from forwarding the messages. When users set the self-destruct timer on secret messages, the messages will disappear from both the sender’s and receiver’s devices when the timer expires.
43. Telegram users have the option to create a user name that is displayed to other users. User names are uniquely assigned on a first-come, first-serve basis. Users have the

ability to conceal their user names from others so that they can utilize Telegram anonymously.

44. Based on my training and experience, I know that individuals involved in child pornography and child exploitation offenses have utilized Telegram Messenger to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of offenders utilize Telegram's security features to avoid detection from law enforcement officers.

Other Social Media Applications

45. Grindr is a geospatial networking and online dating application geared towards gay, bisexual, and trans-sexual individuals. The application runs on iOS and Android mobile devices. It uses mobile devices' geolocation data to allow users to locate other nearby users.
46. WhatsApp is a freeware, cross-platform messaging and Voice over IP (VoIP) service owned by Facebook Inc. It allows users to send text messages and voice messages; make voice and video calls; and share images, documents, user locations, and other media. WhatsApp's client application runs on mobile devices but is also accessible from desktop computers that are connected to the Internet.
47. Based on my training and experience, I know that individuals involved in child pornography and child exploitation offenses have utilized various social media applications, including Grindr, WhatsApp, and Facebook, to trade child pornography files and to communicate with other offenders and victims.

Collectors of Child Pornography

48. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have

companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

- c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

FACTS SUPPORTING PROBABLE CAUSE

- 49. Beginning in or around December 2019, I have been involved in an investigation of child pornography offenses committed by an adult male who will be referred to for purposes of this Affidavit as “Adult Male A”. On or around January 9, 2020, a federal search warrant was executed at Adult Male A’s residence in Dayton, Ohio. Various electronic media

were seized pursuant to the search warrant, including an Apple iPhone. A subsequent search of the iPhone revealed that Adult Male A had utilized the Telegram and WhatsApp Messenger applications to trade child pornography files with others and to discuss the sexual exploitation of children.

50. During the execution of the search warrant, Adult Male A agreed to be interviewed. I have also conducted several follow-up interviews of Adult Male A in or around January 2020. During these interviews, Adult Male A admitted that he utilized the Telegram Messenger application to trade child pornography files with others. Adult Male A identified that one of these individuals was an adult male who lived in or near Piqua, Ohio. Although Adult Male A could not recall this man's name, Adult Male A identified the man via photograph as HALL. Below is a summary of information that Adult Male A provided about HALL during the various interviews:
- a. Adult Male A met HALL on the Grindr online dating application approximately one to two years ago, when Adult Male A was living in Piqua, Ohio. Prior to meeting HALL, Adult Male A had not been involved in child pornography offenses. HALL was the first person who sent Adult Male A child pornography files.
 - b. HALL first talked to Adult Male A about child pornography on the Grindr application. HALL then instructed Adult Male A to download the Telegram application, and they then began communicating on Telegram.
 - c. HALL sent Adult Male A images and videos depicting child pornography on the Telegram application. The children depicted in the child pornography files ranged from infant and toddler ages to teenagers. Adult Male A estimated that HALL sent Adult Male A these child pornography files on less than twenty-five occasions. HALL also invited Adult Male A into a group chat on Telegram that exchanged numerous child pornography files. New members could only be added into this group if they were invited into the group by another member.
 - i. Based on my training and experience, I know that some group chats on online messenger applications will only accept new members if existing members invite the new members into the group. In my experience, this provides an added security feature to ensure that the new members are not affiliated with law enforcement.
 - d. HALL sometimes came over to Adult Male A's residence in Piqua, Ohio so that they could engage in sexually explicit conduct with each other. There were times when HALL watched videos depicting child pornography that he had on his cellular telephone while engaging in the sexual activities with Adult Male A.

Adult Male A was able to see these videos and noted that they depicted HALL engaging in sexually explicit conduct with a male child. Conduct that Adult Male A observed in these videos included HALL touching and fondling the child's buttocks and/or genitals, the child touching HALL's buttocks and/or genitals, HALL providing oral sex to the child, and HALL receiving oral sex from the child.

- i. Based on Adult Male A's descriptions of these videos, I believe that some or all of them depict child pornography. Given that HALL is depicted in the videos, it is reasonable to believe that he produced the videos.
- e. Adult Male A first stated that he had seen at least two videos that depicted HALL engaging in sexually explicit conduct with the male child. Adult Male A later estimated that he had seen at least four of these videos. It appeared to Adult Male A that the boy depicted in the videos was approximately nine to ten years of age. Adult Male A could see HALL's face in the videos and felt confident that HALL was in fact depicted in the videos.
- f. Adult Male A advised that HALL might have called the child depicted in the above described videos his nephew. HALL talked about baby-sitting the child on past occasions.
- g. There was a time when Adult Male A met HALL at a Walmart store in or around Piqua, Ohio. HALL arrived at the store in a black truck. Adult Male A got into HALL's truck and saw that HALL had a small laptop with him. HALL showed Adult Male A child pornography files on this laptop. It appeared to Adult Male A that HALL had hundreds of child pornography files that were saved in a folder on the laptop. Adult Male A did not see any files on the laptop that depicted HALL engaging in sexually explicit conduct with children.
- h. Adult Male A stopped communicating with HALL approximately one year ago, when Adult Male A moved out of his residence in Piqua, Ohio. Adult Male A has not received child pornography files from HALL since that time. Adult Male A periodically received messages from HALL over the past approximately one year via Grindr and Facebook, but Adult Male A did not respond to the messages. The last message that Adult Male A received was in late January 2020 via Grindr. Adult Male identified that HALL's Grindr profile name at that time was "Nwor".
 - i. Adult Male A showed me HALL's profile picture as well as the message he received from HALL. I noted that the profile picture depicted the face of a white male wearing a hat and sunglasses. It appeared that HALL was the individual depicted in the photograph (although the hat and sunglasses prevented a more definitive identification).

- i. HALL was previously on the Friends List of Adult Male A's Facebook account. Adult Male A could not recall HALL's Facebook account name.
 - j. Adult Male A provided a description of HALL that is consistent with HALL's physical appearance. Adult Male A was shown a photograph of HALL, and Adult Male A confirmed that the individual depicted in the photograph was HALL.
 - k. Adult Male A never communicated with HALL via telephone, and Adult Male A did not know HALL's telephone number.
 - l. Adult Male A had never been to HALL's residence. Based on HALL's comments, Adult Male A believed that HALL lived in Piqua, Ohio with a relative.
51. On or around November 29, 2019, an adult male who will be referred to for purposes of this Affidavit as "Adult Male B" submitted an online tip to the FBI's National Threat Operations Center (the FBI's telephone and online complaint system). Adult Male B reported that he recently met a man on the Grindr dating application, and that this man talked about molesting his nephew. I later conducted two interviews of Adult Male B in or around December 2019 and January 2020. Adult Male B reported that he knew the man he met on Grindr as "Teddy" (a common nickname for HALL's middle name, and similar to HALL's known alias, as detailed below). Adult Male B also positively identified HALL from a photographic lineup. The information that Adult Male B provided about HALL during the interviews is consistent with the information provided by Adult Male A. At this time, I am not aware of Adult Male A and Adult Male B being acquainted with each other.
52. In summary, Adult Male B provided the following information about HALL in his online complaint and during the two interviews:
- a. Adult Male B met HALL in or around November 2019 on the Grindr dating application. HALL offered to provide drugs to Adult Male B, and they coordinated to meet with each other. HALL picked up Adult Male B in a dark blue truck (similar to the vehicle Adult Male A saw HALL drive to the Walmart store, as detailed above). While they were in a parking lot, HALL and Adult Male A used a quantity of methamphetamine that HALL provided. HALL then drove Adult Male A to HALL's residence in Piqua, Ohio.
 - b. While at the residence, HALL took Adult Male B to a bedroom on the second floor. It was Adult Male B's understanding that this was HALL's bedroom.

HALL and Adult Male B used an additional quantity of methamphetamine while in the bedroom, which was again provided by HALL.

- c. HALL and Adult Male B engaged in sexual activities with each other in the bedroom. HALL also showed Adult Male B pornographic videos on HALL's cellular telephone. It appeared that HALL played or streamed these videos from a commercial website. HALL commented that he thought that some of the individuals depicted in the videos were juveniles, as he had seen them on the "dark web".
- d. HALL made a number of sexually explicit comments about his nephew during the time that Adult Male B was at the residence. Comments that HALL made about his nephew included the following:
 - i. HALL indicated that he had been sexually active with his nephew for around five years. HALL also indicated that he had regular contact with his nephew.
 - ii. HALL made comments indicating he had provided oral sex to the nephew and that the nephew had provided oral sex to him.
 - iii. HALL said that his nephew had masturbated in front of him.
 - iv. HALL said that he "collected" things from his nephew.
 - v. HALL stated that he had several photographs depicting his nephew nude, but that he would only show Adult Male B one of these photographs.
- e. HALL showed Adult Male B a photograph on HALL's cellular telephone. This photograph depicted a nude male child kneeling on his knees with his buttocks in the air. HALL said that the boy depicted in the photograph was his nephew. Adult Male B advised that based on the angle that the picture was taken, it was difficult to estimate the age of the boy depicted in the photograph. However, it appeared to Adult Male B that the individual depicted in the photograph could possibly be around sixteen to eighteen years of age.
- f. HALL showed Adult Male B a pair of children's underwear that was on the dresser in the bedroom. HALL said that this underwear belonged to his nephew. The underwear appeared to be a size for a male child who was approximately six to eight years of age.
- g. Adult Male B questioned HALL about HALL's possible sexual contact with children. Adult Male B asked if children were sexually different from adults, and

HALL responded that they were. HALL commented that children also tasted differently. HALL made comments about wanting to “rape a young straight boy’s ass” (or words to that effect) and to “eat a baby’s ass” (or words to that effect).

- h. As Adult Male B continued to ask HALL questions, HALL seemed to become paranoid. HALL then told Adult Male B to leave the house.
- i. Approximately one month after meeting HALL, Adult Male B and HALL again communicated with each other via Grindr. Adult Male B met HALL again at HALL’s residence. They used methamphetamine together in HALL’s bedroom, but they did not engage in sexual activities with each other or talk about HALL’s nephew.
- j. Around mid-January 2020, Adult Male B sent HALL a message on Grindr asking how HALL was doing. HALL provided a curt response.
- k. HALL and Adult Male B only communicated with each other via Grindr. Adult Male B did not know HALL’s telephone number or Facebook account name.
- l. Based on comments that HALL made, it was Adult Male B’s understanding that HALL lived with his father. Adult Male B did not meet or see the father at the residence.
- m. During an interview on or around January 30, 2020, Adult Male B accessed and showed me HALL’s Grindr profile picture.
 - i. I noted that HALL’s profile name was “Nwor”, and that it contained the same profile name and picture that Adult Male A had showed to me during one of his interviews (which was a few days prior).
- n. Based on the description that Adult Male B provided of HALL’s residence, Adult Male B was shown various photographs of residences that were in this geographic location. Adult Male B identified that photograph depicting 1435 Covington Avenue in Piqua, Ohio (hereinafter referred to as the “SUBJECT PREMISES”) was HALL’s residence.
- o. HALL made a comment on one occasion that he was employed as a bartender at the Masque night club in Dayton, Ohio
- p. Adult Male B was shown a photographic lineup depicting six white males, one of whom was HALL. Adult Male B positively identified HALL from this lineup.

53. Records from the Ohio Bureau of Motor Vehicles identified that HALL utilized the SUBJECT PREMISES when renewing his Ohio driver's license in 2016. His license was suspended in 2017 and has not been reinstated since that time. Records from the Miami County Auditor's Office identified that William M. Hall owns the SUBJECT PREMISES. Based on his name and date of birth, it appears that William M. Hall is HALL's father or other relative.
54. Records from the Montgomery County (Ohio) Jail identified that HALL was arrested in or around July 2016 for a theft offense and in or around March 2017 for a drug offense. The arresting officers for both arrests noted that HALL's address was the SUBJECT PREMISES when booking him into the jail.
55. As part of the investigation, I obtained a report from the Piqua (Ohio) Police Department regarding suspicious activity at the SUBJECT PREMISES on or around August 12, 2019. According to the report, HALL called 911 from the **TARGET CELL PHONE** and reported that someone had stolen the pump from the swimming pool that was on the property. The report identified that HALL used the name "TED" and that his cellular telephone number was 937-418-2403 (hereinafter referred to as "CELL PHONE-2").
 - a. It was noted that the telephone number that the officer listed for HALL in the report was different from the telephone number that HALL used to call 911. Based on my training and experience, I know the following:
 - i. When writing reports, law enforcement officers sometimes utilize the last known telephone numbers that are documented in the police department's records system if the officers were not able to obtain the person's telephone number during their contact with those individuals.
 - ii. Some individuals own and utilize multiple cellular telephones.
 - iii. In cases where individuals utilize their cellular telephones to conduct illegal activities, it is not uncommon for them to report false cellular telephone numbers to law enforcement officers.
56. Sprint Corporation was identified as the service provider for the **TARGET CELL PHONE**. On or around January 29, 2020, Sprint Corporation was served with a subpoena requesting subscriber information for the **TARGET CELL PHONE**. Records received in response to the subpoena identified that the **TARGET CELL PHONE** was subscribed to William Clemens at an address that is in close proximity to the SUBJECT PREMISES. However, the billing address for the account was the SUBJECT PREMISES. The account was activated on or around September 28, 2019.
 - a. Based on my training and experience, I know that individuals involved in illegal

activities often conceal their identities when signing up for various telephone and Internet accounts. It is not uncommon for such individuals to utilize the names and/or addresses of their spouses, girlfriends/boyfriends, family members, or other associates in order to conceal their identities and/or the locations of their residences.

- b. Also based on my training and experience, I know that some individuals sign up for “family plans” for telephone accounts in order to obtain cost savings. In these cases, the telephone accounts for all individuals on the family plan may be held in one person’s name.
 - c. Furthermore, given that HALL utilized the **TARGET CELL PHONE** to call 911 in August 2019 but the Sprint account was not activated until September 2019, it appears that the **TARGET CELL PHONE** was previously serviced by another telephone provider.
57. Verizon was identified as the service provider for CELL PHONE-2. On or around January 29, 2020, Verizon was served with a subpoena requesting subscriber information for CELL PHONE-2. Records received in response to the subpoena identified that the number belonged to a TracFone¹, and that no subscriber information was maintained by Verizon for the account.
58. On or around February 19, 2020, I reviewed publicly available information on the Facebook website for possible accounts utilized by HALL. I located an account with a profile name of “TED HALL” and an account name of **RitABee78**. Although the current profile picture for the account depicted a generic picture, there were numerous former profile pictures and other photographs posted to the account that depicted HALL. Based on this and other information detailed in the Affidavit, I believe that HALL is the user of the **RitABee78** Facebook account.
59. Consistent with the information provided by Adult Male B, the publicly available profile information for the **RitABee78** Facebook account identified that HALL was formerly employed at the Masque night club. Review of historical information on the account’s publicly available timeline revealed the following information:
- a. On or around November 22, 2015, HALL posted a picture to his account that depicted him and a juvenile male child. This child appeared to be approximately four to six years of age and was wearing pajamas. HALL and the child appeared

¹ TracFone Wireless Inc. is an American prepaid, no-contract mobile phone provider. TracFone Wireless operates as a mobile virtual network operator, holding agreements with other wireless network operators (including Verizon, AT&T Mobility, T-Mobile, Sprint Corporation, and U.S. Cellular) to provide service to its customers.

to be in the kitchen of a residence. HALL posted the following caption with the picture: "My nephew [*male name*]! This boy is growing so fast!!!".

- b. On or around December 14, 2015, HALL changed the profile picture for his account. The new profile picture depicted HALL and the same juvenile male child from the pictured posted on or around November 22, 2015. The child was wearing what appeared to be the same pajamas from the previous photograph, and HALL and the child appeared to be in the same kitchen.
 - c. Another user utilizing the Facebook display name of "William Clemens" (the name of the subscriber for the **TARGET CELL PHONE**) had posted comments to HALL's Facebook account on at least one occasion.
60. As detailed above, approximately one to two years ago, Adult Male A observed child pornography videos on HALL's cellular telephone that depicted HALL engaging in sexually explicit conduct with a male child who appeared to be approximately nine to ten years old. Adult Male A believed that HALL referred to this child as HALL's nephew, and HALL talked about babysitting the child. Also as detailed above, HALL posted pictures of his purported nephew on his Facebook account in November and December 2015 (a few years prior to the child pornography videos Adult Male A observed on HALL's cellular telephone), and this boy appeared to be approximately four to six years old at that time. Based on this and other information detailed in the Affidavit, it is reasonable to believe that the child depicted on HALL's Facebook account might also be the same child depicted in the child pornography videos that Adult Male A observed on HALL's cellular telephone.
61. On or around February 20, 2020, Facebook Inc. was served with a subpoena requesting subscriber information for the **RitABee78** Facebook account as well as logs of IP addresses utilized to access the account. Review of these records provided the following information:
- a. The account was created on or around January 24, 2009, in the name of "TED HALL". The email address of wtedh78@yahoo.com was the registered email address for the account.
 - b. The following cellular telephone numbers were associated with the **RitABee78** Facebook account: **TARGET CELL PHONE**, CELL PHONE-2, 937-214-0594 (hereinafter referred to as "CELL PHONE-3"), and 937-418-8611 (hereinafter referred to as "CELL PHONE-4"). Facebook Inc.'s records identified that these numbers were "verified" in that the account user had responded to text messages that Facebook Inc. had sent to the user.

- c. Facebook Inc. provided a log of IP addresses that had been utilized to log into and out of the **RitaBee78** Facebook account during the approximate time period of July 13, 2019 through February 18, 2020. This log identified that from approximately October 17, 2019 through February 18, 2020, the only IP addresses utilized to access the **RitaBee78** Facebook account were IP addresses serviced by Sprint Corporation and Charter Communications. The use of IP addresses serviced by Sprint Corporation is consistent with someone using the data plan from his/her cellular telephone to access his/her Facebook account. The use of IP addresses serviced by Charter Communications is consistent with someone using wireless Internet service at a residential or business location to access his/her Facebook account.
 - i. As detailed above, Sprint Corporation is the service provider for the **TARGET CELL PHONE**. The investigation has determined that AT&T is the service provider for CELL PHONE-3, and Verizon is the service provider for CELL PHONE-2 and CELL PHONE-4. Based on the logs of IP addresses provided by Facebook Inc. as well as other information detailed in the Affidavit, it is reasonable to believe that HALL is presently using the **TARGET CELL PHONE** to access his Facebook account as well as other Internet accounts.
 - d. The log of IP addresses identified that from approximately July 13, 2019 through September 22, 2019, the only IP addresses utilized to access the **RitaBee78** Facebook account were IP addresses serviced by AT&T Mobility and Charter Communications. The use of IP addresses serviced by AT&T Mobility is again consistent with someone using the data plan from his/her cellular telephone to access his/her Facebook account.
 - i. Based on the log of IP addresses provided by Facebook Inc. and other information detailed in the Affidavit, it is reasonable to believe that HALL previously utilized a cellular telephone that was serviced by AT&T and he currently utilizes a cellular telephone serviced by Sprint Corporation. This information is consistent with the records from Sprint Corporation, which identified that the **TARGET CELL PHONE** was activated on Sprint's network on or around September 28, 2019 (as detailed above).
62. On or around February 21, 2020, a subpoena was served to AT&T requesting subscriber information for CELL PHONE-3. Records received in response to the subpoena identified that the financial and billing party for the account was William Clemens, and the user name for the account was "God God". The address listed for both William Clemens and "God God" was the SUBJECT PREMISES. The email address listed for both William Clemens and "God God" was wtedh78@yahoo.com. The account was

cancelled on or around October 27, 2019 (consistent with the IP logs provided by Facebook Inc.).

63. On or around February 21, 2020, a subpoena was served to Verizon for CELL PHONE-2. Records have not been received from Verizon as of this time.
64. On or around February 21, 2020, an FBI investigator searched publicly available information on the Telegram application for accounts associated with the **TARGET CELL PHONE**, CELL PHONE-2, CELL PHONE-3, and CELL PHONE-4. The investigator found that there were Telegram accounts associated with the **TARGET CELL PHONE** and CELL PHONE-3. The Telegram account associated with the **TARGET CELL PHONE** had a display name of “TED HALL”, and it was presently offline. The Telegram account associated with CELL PHONE-3 had a display name of “Marshall78 HaWl”.
 - a. As detailed above, Adult Male A identified that he previously communicated with and received child pornography files from HALL via Telegram.
65. Based on all of the information detailed in the Affidavit, I submit that there is probable cause to believe the following:
 - a. HALL has engaged in sexually explicit conduct with his nephew and has produced child pornography depicting this conduct. Evidence of this production of child pornography is contained on one or more of HALL’s cellular telephones.
 - b. HALL has utilized the Telegram application to distribute and receive child pornography files. He has utilized at least two cellular telephone numbers (including the **TARGET CELL PHONE**) to access his Telegram accounts.
 - c. HALL has possessed child pornography files on at least two devices – that being his cellular telephone and a laptop computer.
 - d. HALL is the user of the “Nwor” Grindr account. HALL has utilized the Grindr dating website to meet at least some of the individuals to whom he has distributed child pornography files and with whom he has discussed the sexual exploitation of children.
 - e. HALL is the user of the **RitABee78** Facebook account, and he has utilized this Facebook account to post pictures of his nephew. He has also utilized this Facebook account to contact at least one of the individuals to whom he distributed child pornography files (that being Adult Male A). As detailed above, the Facebook account contains at least two pictures depicting what appears to be HALL’s nephew. Based on all of the information detailed in the Affidavit, it is

reasonable the **RitABee78** Facebook account contains information about the victims and co-conspirators of HALL's child pornography activities.

- f. HALL presently uses the **TARGET CELL PHONE**. He has utilized the **TARGET CELL PHONE** as recently as on or around February 18, 2020 to access his Facebook account. He has utilized the **TARGET CELL PHONE** as recently as on or around January 30, 2020 to access his Grindr account.
- g. HALL is the user of the wtedh78@yahoo.com email account, and he has utilized this email account to register his Facebook account as well as potentially other social media accounts that contain evidence of his child exploitation activities.

Evidence Available in Searches of Cellular Telephone Records

- 66. In my training and experience, I have learned that Sprint Corporation is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.
- 67. Based on my training and experience, I know that Sprint Corporation can collect cell-site data about the **TARGET CELL PHONE**. I also know that Sprint Corporation collects additional data called Per Call Measurement Data (PCMD). PCMD was developed to aid in improving cellular service in a particular area. It can measure the time it takes a signal to leave a cellular handset and then return back to the tower. Furthermore, I know that wireless providers such as Sprint Corporation typically collect and retain cell-site data and PCMD pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.
- 68. Based on my training and experience, I know that wireless providers such as Sprint Corporation typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone

service. I also know that wireless providers such as Sprint Corporation typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the **TARGET CELL PHONE**'s user or users and may assist in the identification of co-conspirators and/or victims.

69. As detailed above, there is probable cause to believe that HALL has utilized one or more cellular telephones (to include the **TARGET CELL PHONE**) of his child pornography activities. Cell site and cell sector information for the **TARGET CELL PHONE** on the dates and times that the child pornography files were possessed, received, distributed, and produced could be materially relevant in identifying and/or corroborating the locations where these activities transpired.
70. Furthermore, based on my training and experience, I know that location information from cellular telephones can be materially relevant in investigations involving child exploitation offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims. Data regarding the subjects' whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place. Furthermore, data regarding the subjects' whereabouts as obtained from the location information can lead to the identification of the places where computer devices used in furtherance of the crime may be present.
71. Also based on my training and experience, I know that subscriber information and billing records maintained by telephone providers provide material evidence of criminal offenses. Such information is significant in that it helps in determining the identities of the users of the telephones.
72. Based on the information detailed above, I submit that there is probable cause to believe that the information stored by Sprint Corporation for the **TARGET CELL PHONE** contains evidence of the criminal violations identified above.

Evidence Available in Social Media and Messenger Accounts

73. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

74. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
75. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.
76. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.
77. Based on my training and experience, I know that some individuals routinely utilize Facebook's messenger application to communicate with their associates. I also know that individuals frequently post photographs of their associates, their residences, and their whereabouts on their Facebook accounts. These messages and photographs can provide material evidence regarding the identities of the Facebook user's co-conspirators and/or the locations of the Facebook user's criminal activities.
78. Also as noted above, social media and online chat providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.
79. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers'

billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child pornography, child exploitation, and child sex trafficking offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.

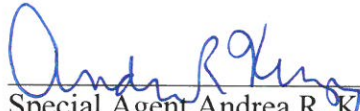
80. Social media and online chat providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.
81. Based on all of the information detailed above, there is probable cause to believe that information associated with the **RitABee78** Facebook account and the wtedh78@yahoo.com email account may contain evidence of HALL's child pornography and child exploitation activities.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

82. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Sprint Corporation, Facebook Inc., and Oath Holdings Inc. to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 through B-3. Upon receipt of the information described in Section I of Attachments B-1 through B-3, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-3.

CONCLUSION

83. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located in the accounts described in Attachments A-1 through A-3, including the following offenses: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), and 2251(a) and (e).
84. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-3.
85. Because the warrants for the accounts described in Attachments A-1 through A-3 will be served on Sprint Corporation, Facebook Inc., and Oath Holdings Inc., who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 25th of February 2020


MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

